UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/668,109	09/22/2003	Ram Anati	36437	7640

67801 7590 09/24/2009

MARTIN D. MOYNIHAN d/b/a PRTSI, INC.
P.O. BOX 16446
ARLINGTON, VA 22215

EXAMINER	
RAHIM, MONJUR	

ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
09/24/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/668,109	ANATI ET AL.	
	Examiner	Art Unit	
	MONJOUR RAHIM	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 June 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the amendment and argument field on 8 June 2009.

2. **Claims 1-42** remain rejected.

3. **Claims 1, 18, 21, 24, 26,** and **31** are amended.

4. **Claims 37-42** are newly added.

Responses to the Argument

5. The applicant's arguments filed on 8 June 2009 have been fully considered but they are not persuasive. In the Remarks, the applicant has argued in substance:

Argument (Page 1-3)

(a) "Atkinson teaches a method for network authentication of a host whereby a sending host (hostA) is verified by a receiving host (hostB) or by an intermediate router or gateway, such that "host b will...verify the authenticity of hostA." As discussed in detail in the patent (column 9, line 36; and column 10, line 8), data provided by hostA may be decoded by hostB, in order to verify the authenticity of hostA. This is shown in the appended fig. 3, at ref. nos. 16' and 88. In the case of intermediate authentication (column 11, lines 10 and 62), data provided by hostA is utilized by an intermediate router, as well as by hostB, to verify the authenticity of hostA. This is shown in the appended fig. 4, at ref. nos. 16, 106, and 124. Atkinson does not teach verifying the authenticity of a user. In contrast, amended Claim 1 recites "A method of authenticating, using an authentication server, the use of an authentication device by at least a first user over a communication network via an intermediate communication device".

(b) "Yet further in contrast to the teachings of Atkinson, amended Claim 26 recites a method of remote validation of at least a first user," including "outputting a validation signal for the first user".

(c) "Said authentication server for authentication of the first user, in contrast it is the method of Authentication of the vendor".

(d) "Authentication server for authentication of the first user".

(e) "Additionally, neither Atkins nor Daudelin teach the limitation found in independent claim 31, "A method of detecting a transmission of an acoustic multitone Frequency Shift key".

(f) *Motivation statement: "While the Examiner has stated that, since encryption coding is a well-known practice, "the skilled person would have been motivated to use such algorithm to communicate efficiently and securely in a distributed environment," the*

Examiner has produced no prior art reference that teaches authenticating the use of an authentication device by at least a 1st user".

Response:

(a) Atkinson teaches user and application level distributed Key. So, Host authenticity is checked by router before authenticate the user in the system and Atkinson clearly mentioned providing user access using asymmetric key (please see col 7, lines 16-20).

(b) Validity of user is determined by the output of the "digital signature", this digital signature is the validation signal (Please see col 8, lines 11-18).

(c) Authenticating vendor is the authenticating users and where vendor is the user per Atkins.

(d) Vendors who request to login, the first waiting in "login queue" in order to login is the first user.

(e) Atkinson does not explicitly teach particular limitation; however Daudelin used a FSK demodulator to detect transmission of Frequency of Shift Key (FSK), please see Daudelin, col 3, lines 9-10.

(f) It is not required to have motivational statement from the reference; however citation from reference has been pin-pointed.

Argument (Page 3-6):

(a) Applicant attached the drawing of prior-art.

Response:

(a) It has been acknowledged by the Examiner.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-8, 17-30 are rejected under 35 U.S.C 102(b) as being anticipated by Atkinson (US Patent No. 5511122), hereinafter Atkinson.

As per **claim 1**, Atkinson discloses:

- **receiving an authentication datagram by said intermediate device, said authentication datagram including data from the user** (Atkinson, col 7, lines 1-25), wherein user's login request, "key" must be embedded in the request , otherwise it would be invalid call. This key is the part of "authentication data" that has included in the request. This Key is interpreted as data-gram.

- protecting said datagrarn by said intermediate device, by at least one of changing, adding to, encrypting and signing of said datagram (Atkinson, col 10, lines 26-33, and col 8, lines 11-18), wherein "key" is encrypted and "digitally signed", as claimed.

- Forwarding said datagram to said authentication server for authentication of the user (Atkinson, col 2, lines 46-49, col 7, lines 1-25), wherein user datagram is sent to the authentication system and this authentication system is the authentication server.

As per **claim 2**, claim 1 is incorporated and further Atkinson discloses:

- **wherein said intermediate device comprises a vendor world wide web site** (Atkinson, col 1, lines 7-12), wherein "distributed network" is the "world wide web", As claimed.

As per **claim 3**, claim 2 is incorporated and Atkinson further discloses:

- wherein protecting comprises adding a signature associated with said vendor to said datagram (Atkinson, col 10, lines 26-33, and col 8, lines 11-18), wherein "key" is encrypted and "digitally signed", as claimed.

As per **claim 4,** claim 2 is incorporated and Atkinson further discloses:

- wherein protecting comprises encrypting said datagram(Atkinson, col 9, lines 1-8), wherein data gets encrypted for security/protection purpose.

As per **claim 5,** claim 1 is incorporated and Atkinson further discloses:

- wherein said intermediate device comprises a user computing device (Atkinson, col 9, lines 26-30), where communication device is computing device.

As per **claim 6,** claim 5 is incorporated and Atkinson further discloses:

- wherein said computing device adds a time stamp to said datagram (Atkinson, col 11, lines 17-24), where timestamp is inherent.

As per **claim 7,** claim 5 is incorporated and Atkinson further discloses:

- wherein said computing device adds a time stamp to said datagram (Atkinson, col 11, lines 17-24, "This permits policy-based routing and usage-based accounting to be dependably implemented as illustrated in dashed box 112. Finally, the intermediate router transmits the reassembled packet to the next router or gateway, possibly refragmenting the packet if necessary, see dashed box 114").where timestamp is inherent.

As per **claim 8,** claim 5 is incorporated and Atkinson further discloses:

- wherein said computing device encrypts said datagram (Atkinson, col 8, lines 7-13,A second method is to encrypt the output of a symmetric cryptographic hash function using an asymmetric encryption algorithm. A third method is to use a keyed asymmetric cryptographic hash algorithm. The above three methods have been utilized in the past to provide end-to-end application-layer authentication but have not been used to provide intermediate network authentication.").

As per **claim 17**, claim 1 is incorporated and Atkinson further discloses:

- wherein different communication paths are used for said authentication and for transaction details from a vendor to said authentication (Atkinson, col 2, lines 46-49, "It is still another object of the invention to provide an authentication system in which the first packet

or datagram fragment is dynamically routed while all succeeding packet fragments or datagram fragments then follow the established path of the first packet fragment or datagram fragment").

As per **claim 18**, Atkinson discloses:

- sending an encrypted datagram by secure computer communication from vendor software to said remote authenticator; (Atkinson, col 6, lines 2-9), the recipient is the remote authenticator communicated via vendor software.

- receiving said encrypted datagram by a remote authenticator (Atkinson, col 6, lines 1-9), wherein the recipient is the remote authenticator.

- comparing said datagram or a hash thereof to a hash table at said server (Atkinson, col 2, lines 59-61, "transmitting the signature along with data to a first subnetwork in at least one packet, having a first packet size which is different from that of the transmitting host and thereby fragmenting the original packet into at least two packet fragments"), wherein differentiating of hashed data is comparing, as claimed.

- generating a binary validation answer by said server without an associated explanation (Atkinson, col 7, lines 23-26, "All responses would use IP authentication. The Key Information Protocol would also use the host's public authentication key in the KIP response to enable the recipient to authenticate the response"), wherein response KIP is a binary validation by definition.

- outputting validation answer ((Please see col 8, lines 11-18), wherein Validity of user is determined by the output of the "digital signature", this digital signature is the validation signal

Claim 19 is rejected under the same reason set forth of claim 18 and Atkinson further discloses:

- datagram includes a secret code and wherein said secret code exists only on said authentication device (Atkinson, col 8, lines 62-67), wherein implemented trusted code in the authentication server" is secrete code.

As per **claim 20**, claim 19 is incorporated and further Atkinson discloses:

- Wherein said authentication device includes a plurality of secret codes that are generated to appear unrelated (Atkinson, col 10, lines 30-33), wherein trusted code/cryptographic signature get generated, as claimed.

As per **claim 21**, Atkinson discloses:

- providing a code generating software (Atkinson, col 10, lines 30-33), wherein code generating by the software in inherent.

- providing at least one seed code for said software (Atkinson, col 8, lines 62-67), wherein verify the correctness and trustworthiness of smaller amounts of code than larger amounts of code is seed.

- destroying said seed immediately after generating said code set (Atkinson, col 7, lines 7-15), wherein ignore unauthenticated responses, interpreted as destroying.

-forwarding said code set to said authentication device (Atkinson, col 2, lines 46-49), wherein "dynamically routed data" is the same as forwarding code set, as claimed.

- storing said code set or an indication thereof on an authentication device, Atkinson discloses the generation and utilization of code, inherently has storing capability.

Claims **22 and 23** are rejected under the same reason set forth in connection of claim 18 and 21.

As per **claim 24**, Atkinson discloses:

-generating one time code for the user for the session (Atkinson, col 2, lines 54-57), wherein utilizing the public key from the receiving host in combination with a private key from the sending host to generate a cryptographic signature is the one time code.

- receiving an authentication datagram from said user (Atkinson, col 2, lines 46-49, "It is still another object of the invention to provide an authentication system in which the first packet or datagram fragment is dynamically routed while all succeeding packet fragments or datagram fragments then follow the established path of the first packet fragment or datagram fragment"), where "datagram" is dynamically sending, so inherently other side (Authenticator) is receiving it, as claimed;

- passing on said datagram for verification by a remote authentication server if at least an indication of said one time code that matches said user is provided with said datagram (Atkinson, col 3, lines 10-16), wherein authenticator perform verification of the cryptographic signature on the reassembled packet and utilizing a public key for the sending host to verify the cryptographic signature.

Claim 25 is rejected under the same reason set forth in connection of claim 3.

As per **claim 26,** Atkinson discloses:

- matching said datagram or a hash of said datagram to a table (Atkinson, col 2, lines 59-61), where differentiating the hashed code is comparing, as claimed.

- calculating a counter value from a matching position in said table (Atkinson, col 7, lines 3(Atkinson, *****), wherein generating number of packets are the calculating value, as claimed.

- validating said authentication datagram based on an increase in said counter over a previous counter being within a certain limit (Atkinson, col 3, lines 42-46, "FIG. 4)

- and for each datagram received, outputting a validation signal for the first user (Atkinson, col 7, lines 16-20), Atkinson teaches user and application level distributed Key. So, Host authenticity is checked by router before authenticate the user in the system and Atkinson clearly mentioned providing user assess using asymmetric key.

Claims 27-29 are rejected based on inheritance:

As per **claim 27**, where authentication mechanism based encryption/decryption and it inherently checked or compare for number of try for successful or unsuccessful attempts to identify unwanted visitor.

As per **claims 28-29**, where check for the threshold settings is inherent.

Claim 30 is rejected under the same reason set forth of claim 26 and further "check for the threshold" is inherent.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 9-16, 31-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson (US Patent No. 5511122),), hereinafter Atkinson and further in view of Douglas S. Daudelin (US PAT No. 4716376), hereinafter Daudelin

As per **claims 9-16**:

Official notice is hereby taken it is well-known practice of encryption coding, such as using "temporary code", matching user with session ID, using of ActiveX, embedded software, caching data, secure connection between client and server, use of different path for different types of data (please see PTO-892 FORM, Kurowski, paragraph 0194].

The skilled person would have been motivated to use such algorithm to communicate efficiently and securely in a distributed environment.

As per **claim 31,** Atkinson does not teach "detecting a transmission of an acoustic multitone FSK signal**".** However, Daudelin discloses:

- Detecting a transmission of an acoustic multitone FSK signal (Daudelin, col 3, lines 9-10, "FSK demodulator can optimally detect an FSK signal");

- receiving an acoustic signal (Daudelin, col 12, lines, "The constraints stem from the requirement that the received signal pass through the threshold value as the receiver's input frequencies are changed");

- converting the signal into a Hilbert-transform representation of the signal (Daudelin, col 4, lines, "The output of sampling circuit 160 is also applied on line 2 to a fixed phase shifting circuit 170 which includes a Hilbert transformer 4"), where "transformer 4" is the signal converter, as claimed;

- correlating said converted signal with at least one reference signal representing at least one expected frequency in said FSK signal (Daudelin, col 3, lines 48-56).

- integrating said correlation over an interval (Daudelin, col 2, lines 29-32").

- determining if a signal is present, based on a shareholding of a result of said integrating (Daudelin, col 13 , lines 45-50, "The difference generated by circuit 504 on line 506 is denominated a "threshold adjusted" signal and is applied to a decision circuit 501 which merely determines whether the threshold adjusted signal is positive or negative. The output from circuit 501 on line 500 represents the original FSK encoded data").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching "Authentication mechanism" of Atkinson with FSK and transmitting signal from an "authentication card disclosure Daudelin of transmitting signal from an "authentication card", because each of the versions can be squared and applied to an exclusive OR circuit, the output of which has a d.c. component that allows discrimination between the upper and lower FSK frequencies. It is also to be noted that the use of a multiplier is, however, advantageous, because the effects of the higher order harmonic introduced by that nonlinear operation can be eliminated in a digital signal processing implementation, stated by Daudelin in col 4, lines 60-67.

As per **claim 32**, claim 31 is incorporated and Atkinson does teach "detecting signal". However, Daudelin discloses:

- comprising further determining if a detected signal has a frequency within a certain frequency range (Daudelin, col 3, lines 9-13, "FSK demodulator can optimally detect an FSK signal composed of any two frequencies which lie within a broad range of the two frequencies the demodulator is initially tuned to detect").

As per **claim 33**, claim 31 is incorporated and Atkinson does not teach "detecting signal". However, Daudelin discloses:

- determining if a detected signal has a signal to noise ratio within a certain signal to noise ratio range (Daudelin, col 1, lines 31-42, " FSK input signal is formed which is phase shifted an amount that is a function of the instantaneous signal frequency, and the product of the

original and phase shifted versions is then computed. The product contains a dc component equal to the cosine of the phase difference between the two signals, and a double frequency component. Ideally, the phase difference is chosen to be 90 degrees at the carrier frequency, in order to permit maximum noise immunity").
The same motivation applies as in claim 31, in this claim 33.

As per **claim 34**:

Atkins does not explicitly teach **comprising resampling said signal after said determining;** however in relevant art Daudelin, col 3, lines 60-62, "The input to detector 150 consists of samples of the filtered FSK signal which are obtained by sampling the output of filter 101").
The same motivation applies as in claim 31, in this claim 34.

As per **claim 35**, claim 31 is incorporated and further discloses by Daudelin:

- wherein said threshold is noise dependent of the received signal (Daudelin, col 4, lines, " This arrangement gives the highest degree of noise immunity and also allows the ensuing threshold decision circuit 103 to operate by simply deciding if the value of the signal output from low pass filter 102 is greater or less than zero").
The same motivation applies as in claim 31, in this claim 35.

As per **claim 36**, claim 31 is incorporated and further discloses by Daudelin:

- calculating said interval based on a hardware characteristic of a producer of said acoustic signal (Daudelin, col 13, lines 66-67, and col 14, lines 1-11), where interval was calculated by the circuit, as claimed.
The same motivation applies as in claim 31, in this claim 36.

8. **Claims 37-42** are rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson (US Patent No. 5511122), hereinafter Atkinson and further in view of Douglas S. Daudelin (US

PAT No. 4716376), hereinafter Daudelin and further in view of Schutzer, Daniel (US Patent No. 6873974), hereinafter Schutzer.

As per claim **37**, claim 1 is incorporated and Atkins discloses:

Atkinson does not explicitly teach **wherein said authentication datagram additionally includes data from a second user** however in a relevant art Boreckiet discloses debit or credit card and its information, wherein "credit card/consumer wallet" itself is a second user and inputted card information is additional authentication datagram (Schutzer, Abstract).

- wherein said forwarding includes forwarding said datagram to said authentication server for authentication of the second user (Boreckiet, col 9, lines 35-40), wherein authentication of card information sent to "central server", as claimed.

Same motivation applies herein claim as equally as in claim 1.

As per claim **38**, claim 18 is incorporated and Atkins discloses:

Atkinson does not explicitly teach **wherein said encrypted datagram additionally includes data from a second user** (Schutzer, col 9, lines 35-40), wherein credit card data being encrypted,

- and wherein said outputting additionally includes outputting said validation answer for authentication of the second user (Schutzer, col 10, lines 12-20).

Same motivation applies herein claim as equally as in claim 1.

As per claim **39**, claim 19 is incorporated and Atkins discloses:

Atkinson does not explicitly teach **wherein said encrypted datagram additionally includes data from a second user** however in a relevant art Boreckiet discloses debit or credit card and its information, wherein "credit card/consumer wallet" itself is a second user and inputted card information is additional authentication datagram (Schutzer, Abstract).

- wherein said outputting additionally includes outputting said validation answer for authentication of the second user (Boreckiet, col 10, lines 12-20).

Same motivation applies herein claim as equally as in claim 1.

As per claim **40**, claim 21 is incorporated and Atkins discloses:

Atkinson does not explicitly teach **wherein said remote device is additionally configured for authentication of a second user** (Schutzer, col 1, lines 65-67 and col 2, lines 1-4), where "payment engine" is configured to authenticate credit card. Credit card itself is the second user.

- wherein said providing at least one seed code additionally includes providing at least one seed code for the second user for said software (Schutzer, col 9, lines 35-40), wherein encryption inherently has a seed.

As per claim **41**, claim 26 is incorporated and Atkins discloses:

- wherein said method is additionally for remote validation of a second user (Schutzer, Abstract).

- wherein said receiving additionally includes, from the second user, receiving an authentication datagram by an authentication server from a remote authentication device (Schutzer, Abstract), wherein "credit card umber and address of the user" as the additional datagram form the credit card, And this card itself a second user.

- wherein said outputting additionally includes outputting a validation signal for the second user (Schutzer, col 8, lines 48-58), wherein validity of the validation of second user gets communicated.

As per claim **42**, claim 31 is incorporated and Atkins discloses:

- wherein said at least a first user comprises a first user and a second user (Schutzer, Abstract), wherein "consumer" who is shopping using credit card is the "first and second user" (Schutzer, Abstract).

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure (See form "PTO-892 Notice of reference cited).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MONJOUR RAHIM whose telephone number is (571)270-3890. The examiner can normally be reached on 5:30 AM - 3:30 PM (Mo - Th).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz, Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Monjour Rahim/
Patent Examiner
Art Unit: 2434
Date: 9/13/2009

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434